2.2 Conducting the Internal Control Review

2.2.1 Management is responsible for developing and maintaining internal control activities that comply with the following standards to meet internal control objectives:

• Control Environment,
• Risk Assessment,
• Control Activities,
• Information and Communications, and
• Monitoring

2.2.2 OMB Circular A-123 states that "management should have a clear, organized strategy with well defined documentation processes that contain an audit trail, verifiable results, and specify document retention periods so that someone not connected with the procedures can understand the assessment process."

2.2.3 DOCUMENTING KEY WORK ACTIVITIES: OICs and Center Directors should document internal control activities to show how their significant activities, processes and IT systems are complying with the 5 internal control standards. The following in-depth description of standards should be considered:

2.2.3.1 CONTROL ENVIRONMENT: A positive control environment is the foundation for all other standards. It provides discipline and structure as well as the climate which influences the quality of internal control. Several key factors affect the control environment, including: The integrity and ethical values maintained and demonstrated by management and staff; management's commitment to competence; management's philosophy and operating style including the degree of risk the agency is willing to take; the attitude and philosophy of management toward information systems, accounting, personnel functions, monitoring, and audits and evaluations; the agency's organizational structure for planning, directing, and controlling operations; human capital policies and practices; and the agency's relationship with the Congress and central oversight agencies such as OMB.

2.2.3.2 RISK ASSESSMENT: A precondition to risk assessment is the establishment of clear, consistent control objectives. Risk assessment is the identification and analysis of relevant potential risks associated with achieving the objectives, and forming a basis for determining how risks should be managed. Management needs to comprehensively identify risks and should consider all significant interactions between the entity and other parties as well as internal factors at both the entity-wide and activity levels. Risk identification methods may include qualitative and quantitative ranking activities, management conferences, forecasting and strategic planning, and consideration of findings from audits and other assessments. Once risks have been identified, they should be analyzed for their possible effect. Risk analysis generally includes estimating the risk's significance, assessing the likelihood of its occurrence, and deciding how to manage the risk and what actions should be taken.

2.2.3.3 CONTROL ACTIVITIES: The policies, procedures, techniques, and mechanisms that enforce management's directives, such as the process of adhering to requirements for budget development and execution. Control activities occur at all levels and functions of the entity. They include a wide range of diverse activities such as approvals, authorizations, verifications, reconciliations, performance reviews, maintenance of security, and the creation and maintenance of related records which provide evidence of execution of these activities as well as appropriate documentation. Control activities may be applied in a computerized information system

environment or through manual processes. Activities may be classified by specific control objectives, such as ensuring completeness and accuracy of information processing.
There are certain categories of control activities that are common to all agencies. Examples include the following: top level reviews of actual performance; reviews by management at the functional or activity level; management of human capital; controls over information processing; physical control over vulnerable assets; establishment and review of performance measures and indicators; segregation of duties; proper execution of transactions and events; accurate and timely recording of transactions and events; access restrictions to and accountability for resources and records; and appropriate documentation of transactions and internal control.

Also, there are two broad groupings of information systems control - general control and application control. General control applies to all information systems—mainframe, minicomputer, network, and end-user environments. Application control is designed to cover the processing of data within the application software.

General Control: This category includes entity-wide security program planning, management, control over data center operations, system software acquisition and maintenance, access security, and application system development and maintenance. Data center and client-server operations controls include backup and recovery procedures, and contingency and disaster planning. In addition, data center operations controls also include job set-up and scheduling procedures and controls over operator activities. System software control includes control over the acquisition, implementation, and maintenance of all system software including the operating system, data-based management systems, telecommunications, security software, and utility programs. Access security control protects the systems and network from inappropriate access and unauthorized use by hackers and other trespassers or inappropriate use by agency personnel. Specific control activities include frequent changes of dial-up numbers; use of dial back access; restrictions on users to allow access only to system functions that they need; software and hardware "firewalls" to restrict access to assets, computers, and networks by external persons; and frequent changes of passwords and deactivation of former employees' passwords. Application system development and maintenance control provides the structure for safely developing new systems and modifying existing systems. Included are documentation requirements; authorizations for undertaking projects; and reviews, testing, and approvals of development and modification activities before placing systems into operation. An alternative to in-house development is the procurement of commercial software, but control is necessary to ensure that selected software meets the user's needs, and that it is properly placed into operation.

Application Control: This category of control is designed to help ensure completeness, accuracy, authorization, and validity of all transactions during application processing. Control should be installed at an application's interfaces with other systems to ensure that all inputs are received and are valid and outputs are correct and properly distributed. An example is computerized edit checks built into the system to review the format, existence, and reasonableness of data. Because information technology changes rapidly, controls must evolve to remain effective. Changes in technology and its application to electronic commerce and expanding Internet applications will change the specific control activities that may be employed and how they are implemented, but the basic requirements of control will not have changed. As more powerful computers place more responsibility for data processing in the hands of the end users, the needed controls should be identified and implemented.

2.2.3.4 INFORMATION AND COMMUNICATION: For an entity to run and control its operations, it must have relevant, reliable, and timely communications relating to internal as well as external events. Information is needed throughout the agency to achieve all of its objectives.

Program managers need both operational and financial data to determine whether they are meeting their agencies' strategic and annual performance plans and meeting their goals for accountability for effective and efficient use of resources. Pertinent information should be identified, captured, and distributed in a form and time frame that permits people to perform their duties efficiently. Effective communications should occur in a broad sense with information flowing down, across, and up the organization. In additional to internal communications, management should ensure there are adequate means of communicating with, and obtaining information from, external stakeholders that may have a significant impact on the agency achieving its goals. Moreover, effective information technology management is critical to achieving useful, reliable, and continuous recording and communication of information.

2.2.3.5 MONITORING: Internal control should generally be designed to assure that ongoing monitoring occurs in the course of normal operations. It is performed continually and is ingrained in the agency's operations. It includes regular management and supervisory activities, comparisons, reconciliations, and other actions people take in performing their duties. Separate evaluations of control can also be useful by focusing directly on the controls' effectiveness at a specific time. The scope and frequency of separate evaluations should depend primarily on the assessment of risks and the effectiveness of ongoing monitoring procedures. Separate evaluations may take the form of self-assessments as well as review of control design and direct testing of internal control. Separate evaluations also may be performed by the agency Inspector General or an external auditor. Deficiencies found during ongoing monitoring or through separate evaluations should be communicated to the individual responsible for the function and also to at least one level of management above that individual. Serious matters should be reported to top management.